Grenoble INP Ensimag

Sécurité des réseaux

- **Lecturers**: Fabien Duchene, Dominique Vicard
- Chapters:
  - 4. Intranet
  - 5. protocols, access

Plan (nouveau, sujet à de légères modifications)

- **0. Introduction**
  - Le réseau
  - Parano: mode d'emploi
- **1. Menaces, vuln., attaques**
  - Définitions
  - Attaques
- **2. Qqes algorithmes**
  - Stéganographie
  - Partage de secret
  - P2P: l'algo. Eigentrust
- **3. Poste client**
  - Certifications
  - Principes de la sécurité
  - Principaux méchanismes
  - NT4+
  - Unix
- ***4. Intranet***
  - ***Authentification*** ***Active Directory, Kerberos***
  - ***Conformance*** ***(IDS/IPS, Antimalware, NAC)***
- ***5. Protocoles***
- ***IPSec***
- ***RFID***
- ***RAS: PPTP, L2F, L2TP***
- ***SSL/TLS***
- ***VPN***
- ***EAP & RADIUS***
- ***802.11***
- ***GSM***
- **6. Internet**
  - Pare-feu (Firewall)
  - Proxy, Socks
  - PKI
- **7. Navigateur**
  - Privacy mode
  - Javascript, XSS
  - Flash, ActiveX, Java
  - Sandbox
  - HTLM5

4. Intranet

- **Authentication**
  - Active Directory
  - NT5+: quelques protocoles
  - Kerberos
- **IDS & IPS**
- **Conformance**
  - Antimalware
  - Network Access Control

4.1.1. Active Directory

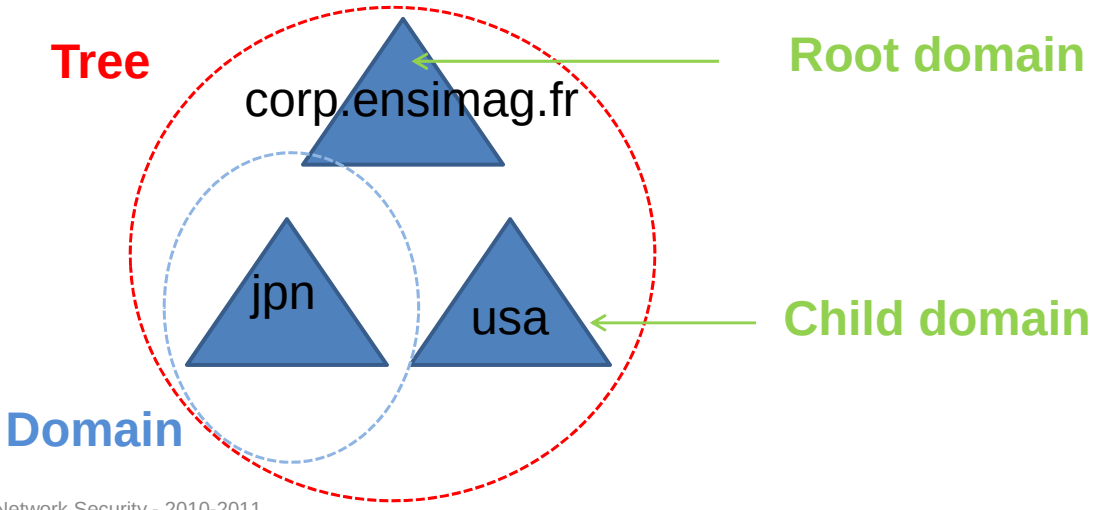
- **Active Directory Directory Services: service d'annuaire:**
  - Ouverture de session unique
  - Accès universel aux ressources
  - Administration centralisée ou déléguée
  - Service d'authentification et de fourniture de données d'authentification
- **Fonctionnalités**:
  - **Kerberos** authentication
  - **LDAP** directory (contains **Security Principals** & other objects)
  - **DNS** resolution
- **Versions**:
  - 2000 native, 2000 mixed ; 2003, 2003 R2 ; 2008, 2008 R2

4.1.1. Rôle de machines Windows

- **Autonome (Workgroup)**
  - Non membre d'un domaine
  - Base de comptes "SAM" (Security Account Manager) locale
- **Client membre (d'un domaine)**
  - Base SAM locale
  - Authentification:
    - domaine
    - SAM locale
- **Contrôleur de domaine (DC)**
  - Copie des objets du domaine
  - Assure le rôle KDC dans Kerberos
    - Authentifie les machines et utilisateurs

4.1.1. ADDS – Domaines, Forêts

- **Domaine (domain):** 1 FQDN DNS, 1 annuaire (security principals, politiques de sécurité), authentification
- **Arbre (tree):** hiérarchie de domaines DNS
- **Forêt (forest):** plusieurs hiérarchies DNS (cf slide suivante)

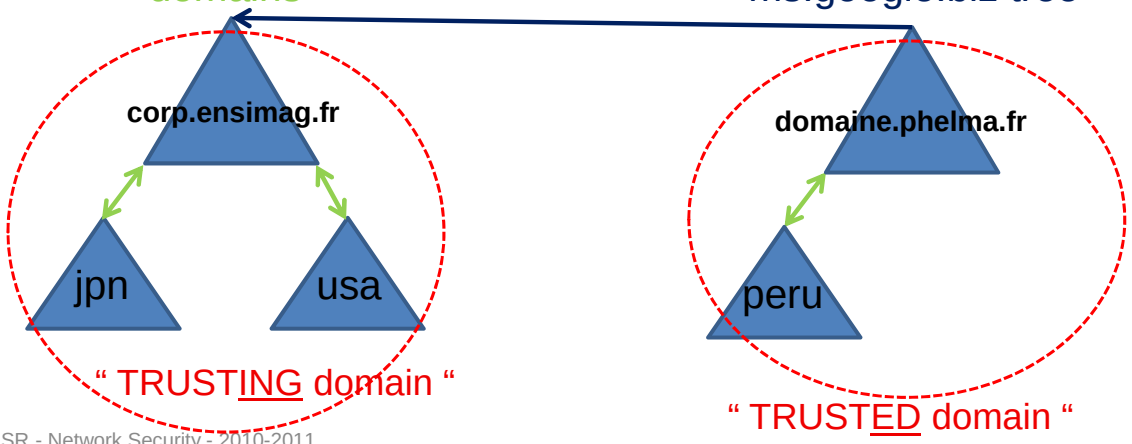


4.1.1. ADDS – relations d'approbations

- Trust relationships
  - **"one-way trust" A<-B:** one way (transitive or not) relation meaning a domain A considers the **identities** provided by B as valid
  - **"two-way trust" A<->B = (A<-B) AND (B<-A)**

Within a tree: implicit transitive 2-way trust between child and parent domains

Example of one-way **forest** trust: corp.nintendo.com **trusts** ms.google.biz tree



4.1.2. Windows NT5+ : quelques protocoles

- **NT5: Windows 2000**
- **Protocoles:**
  - **clé partagés**
    - Authentification **NTLM (domaines hétérogènes)**
    - Authentification **Kerberos V5**
  - **clé publique**
    - Secure Sockets Layer (**SSL**) / transport Layer Security (**TLS**)
    - **IPSec**
- Active Directory peut gérer différents types de **credentials (SSP)**
- **Rôles de machine Windows**

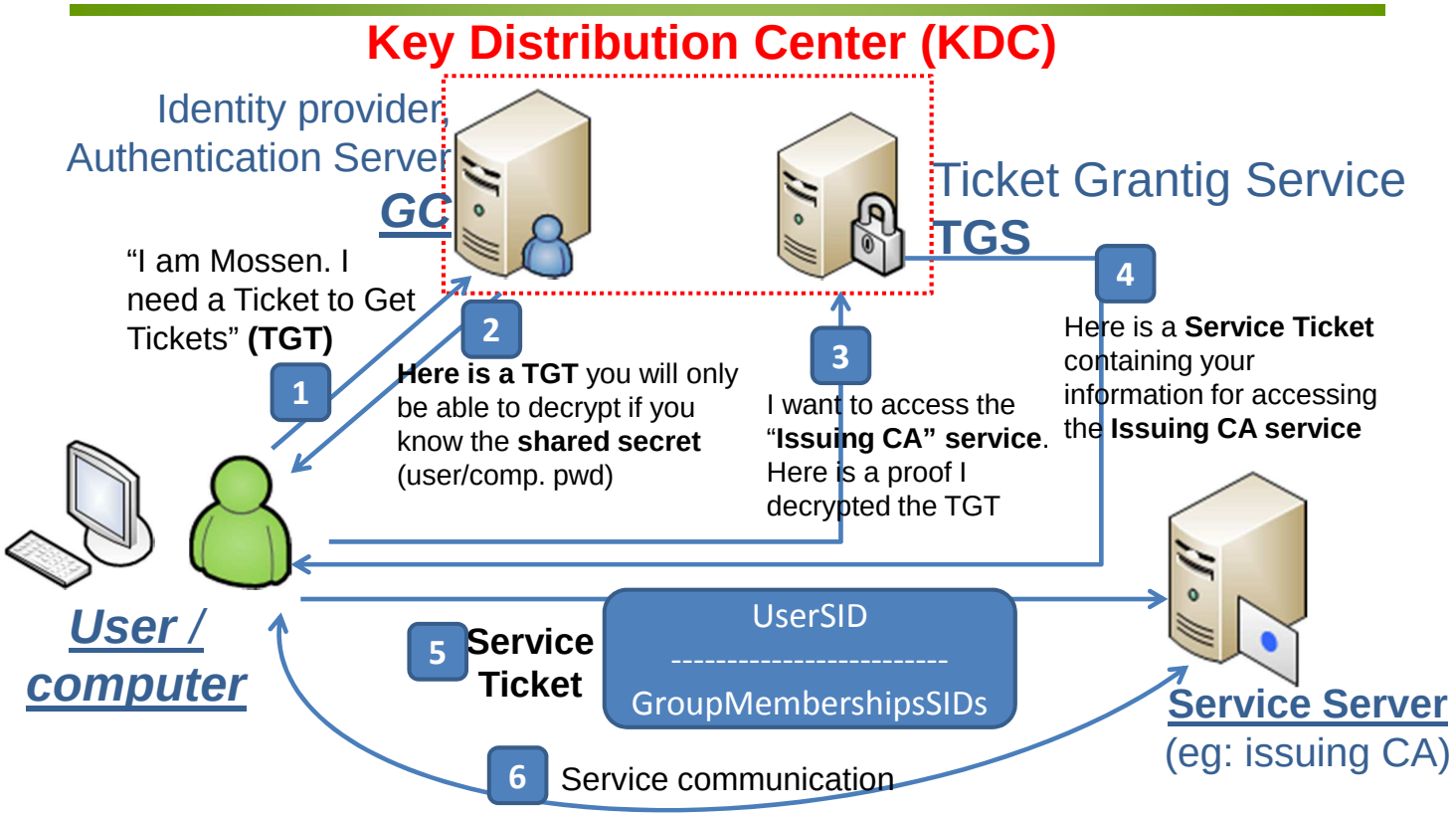
4.1.3. Kerberos

Kerberos & Herakles

(Cerbère & Hercules)

- **Protocole authentification, autorisation, développé par le MIT** (Projet ATHENA), ~ Single-Sign-On
- Version actuelle: v5 RFC4120
- Hypothèse: le réseau peut être non sûr
- Basé sur l'existence d'un **tiers de confiance**, le KDC (« Key Distribution Center »
- **Cryptographie**
  - principlament **symétrique**
  - éventuellement **assymétrique** (eg: auth. par carte à puce)
- **Déclinaisons**:
  - MIT Kerberos
  - **Microsoft Kerberos, Windows NT (>=2000)**
  - Heimdal Kerberos, Suède

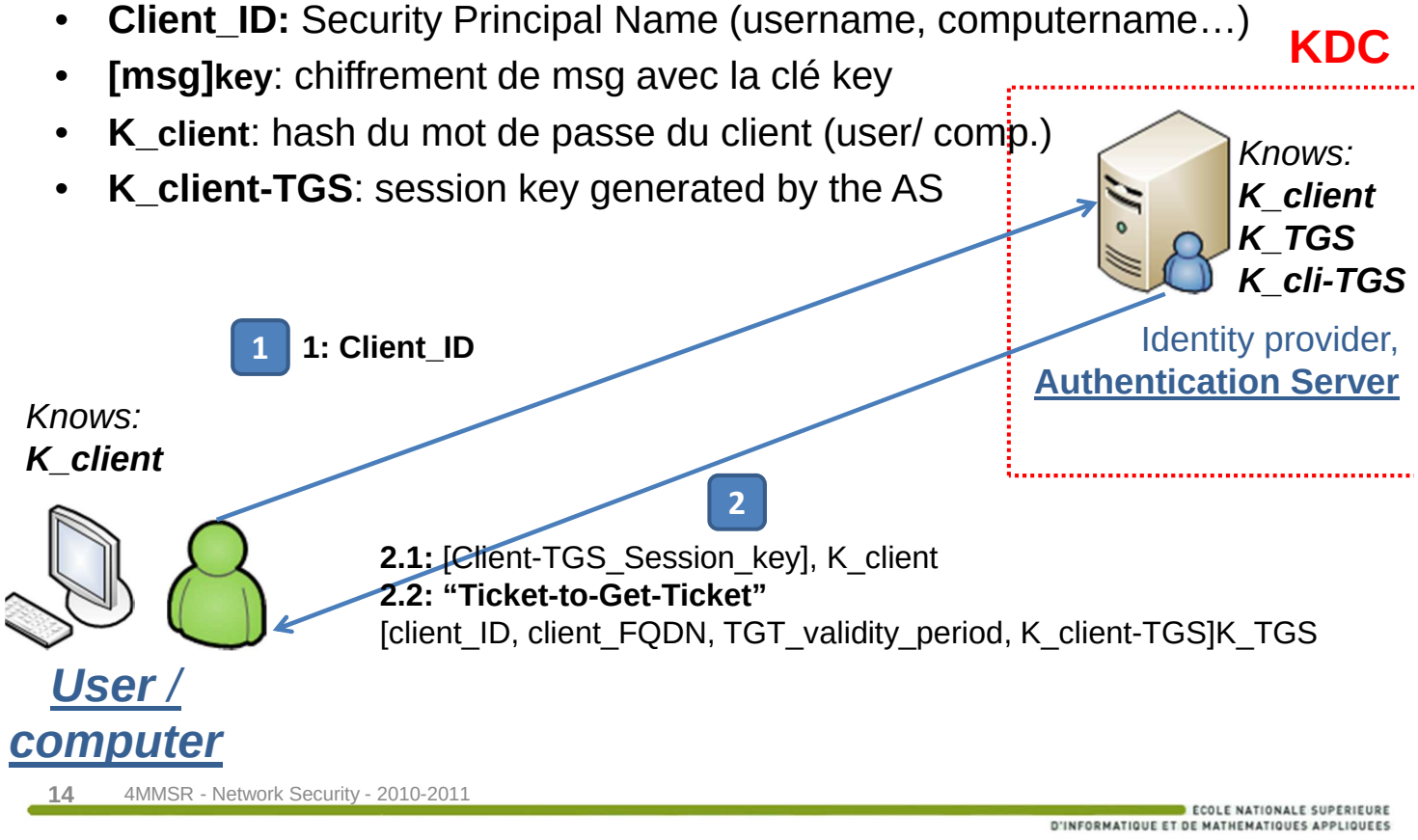
4.1.3. Kerberos: authentication & service access


Key Distribution Center (KDC)
Identity provider
Authentication Server
GC
Ticket Grantig Service
TGS
"I am Mossen. I need a Ticket to Get Tickets" (TGT)
1
2
Here is a TGT you will only be able to decrypt if you know the shared secret (user/comp. pwd)
3
I want to access the "Issuing CA" service. Here is a proof I decrypted the TGT
4
Here is a Service Ticket containing your information for accessing the Issuing CA service
User / computer
5
Service Ticket
UserSID
GroupMembershipsSIDs
Service Server
(eg: issuing CA)
6
Service communication

Introduction to the Microsoft PKI ADCS 2008 R2 (2011), Fabien Duchene, Sogeti-ESEC

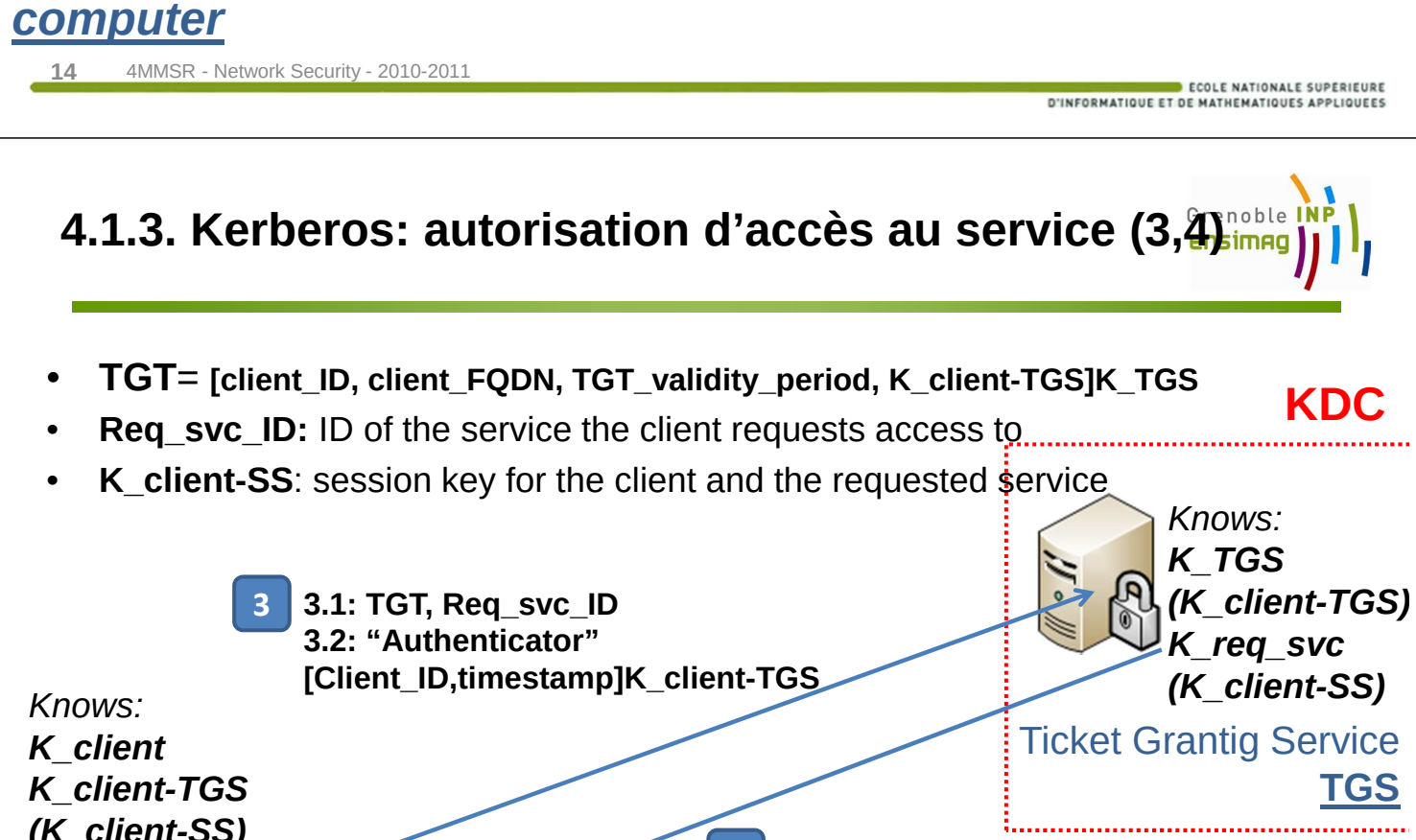
4.1.3. Kerberos: authentification du client (1,2)

- **Client_ID:** Security Principal Name (username, computername…)
- **[msg]key**: chiffrement de msg avec la clé key
- **K_client**: hash du mot de passe du client (user/ comp.)
- **K_client-TGS**: session key generated by the AS



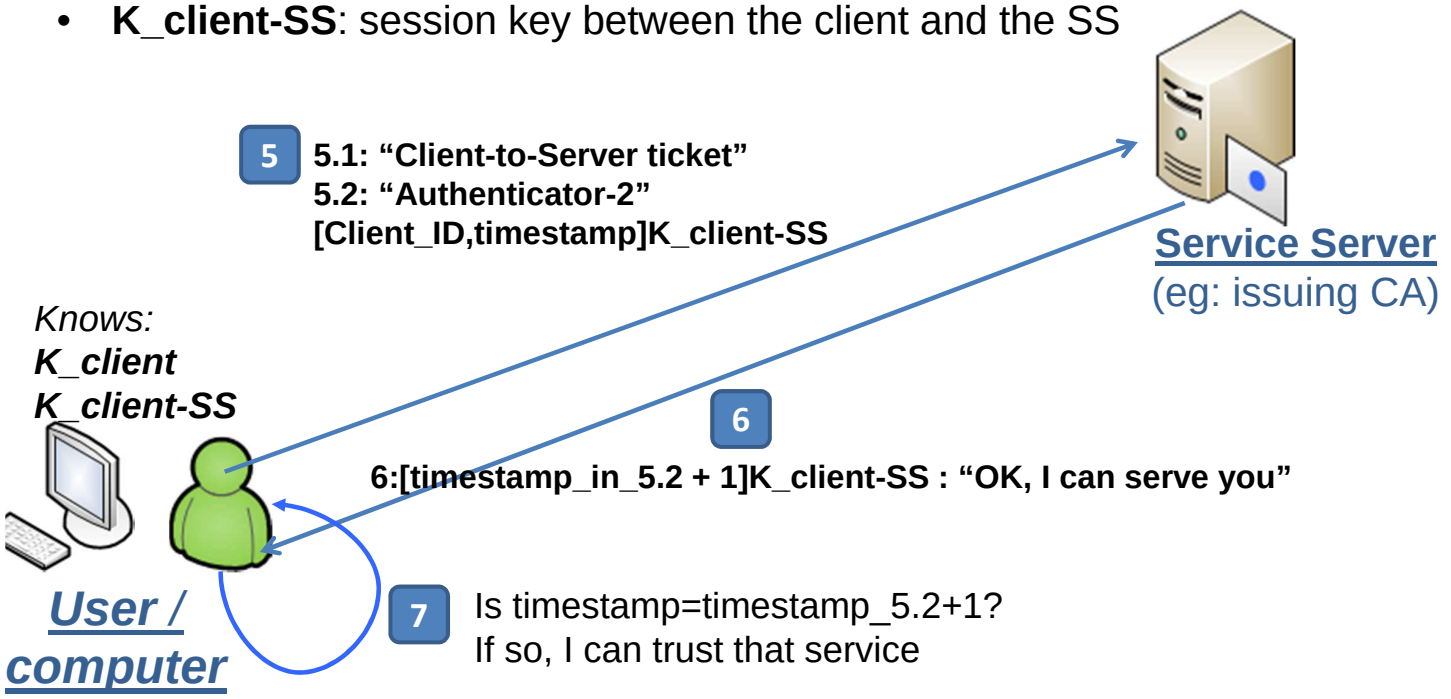
4.1.3. Kerberos: autorisation d'accès au service (3,4)

- **TGT= [client_ID, client_FQDN, TGT_validity_period, K_client-TGS]K_TGS**
- **Req_svc_ID:** ID of the service the client requests access to
- **K_client-SS**: session key for the client and the requested service



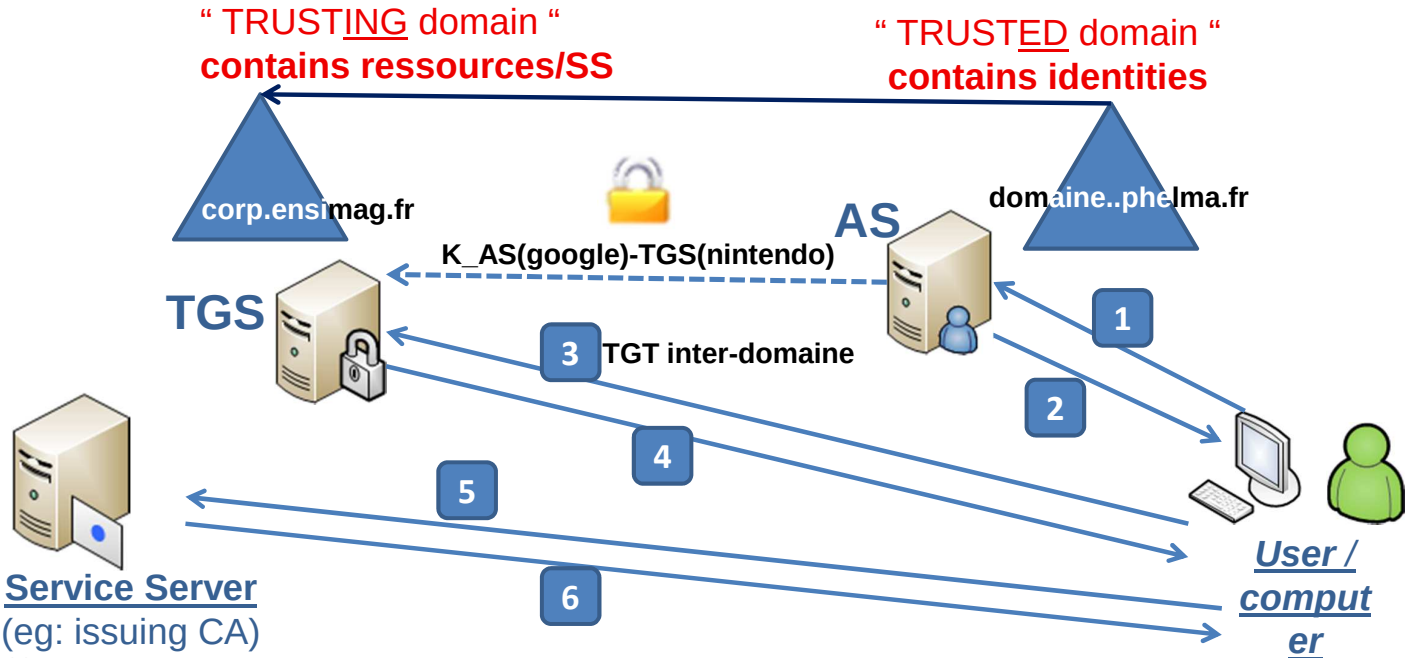
4.1.3. Kerberos: accès au service (5,6)

- **Client-to-Server ticket:**
  [client_ID,client_FQDN,TCS_validity_period,K_client-svc] K_req_svc
- **K_client-SS**: session key between the client and the SS



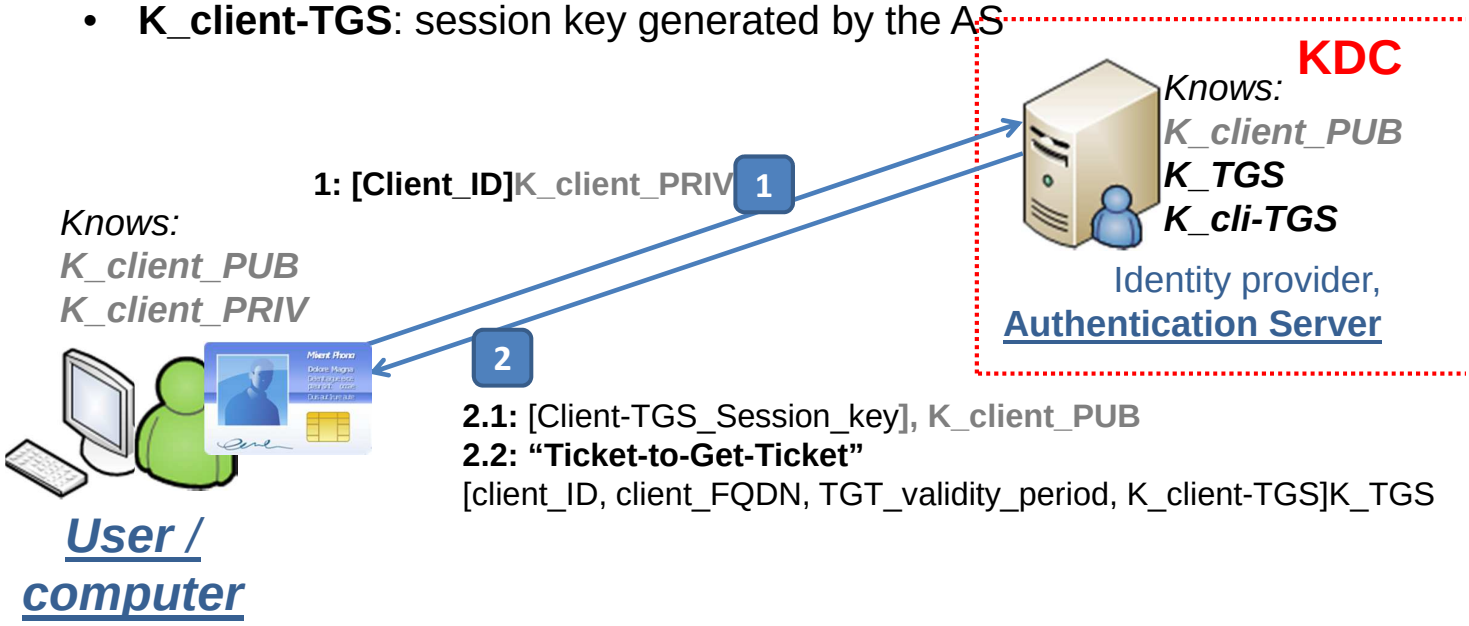
4.1.3. Kerberos – Accès inter-domaine

- Une relation de confiance est établie par le biais d'une **clé partagée** entre domaines, grâce à laquelle des **referals tickets (TGT inter-domaine)** sont envoyés

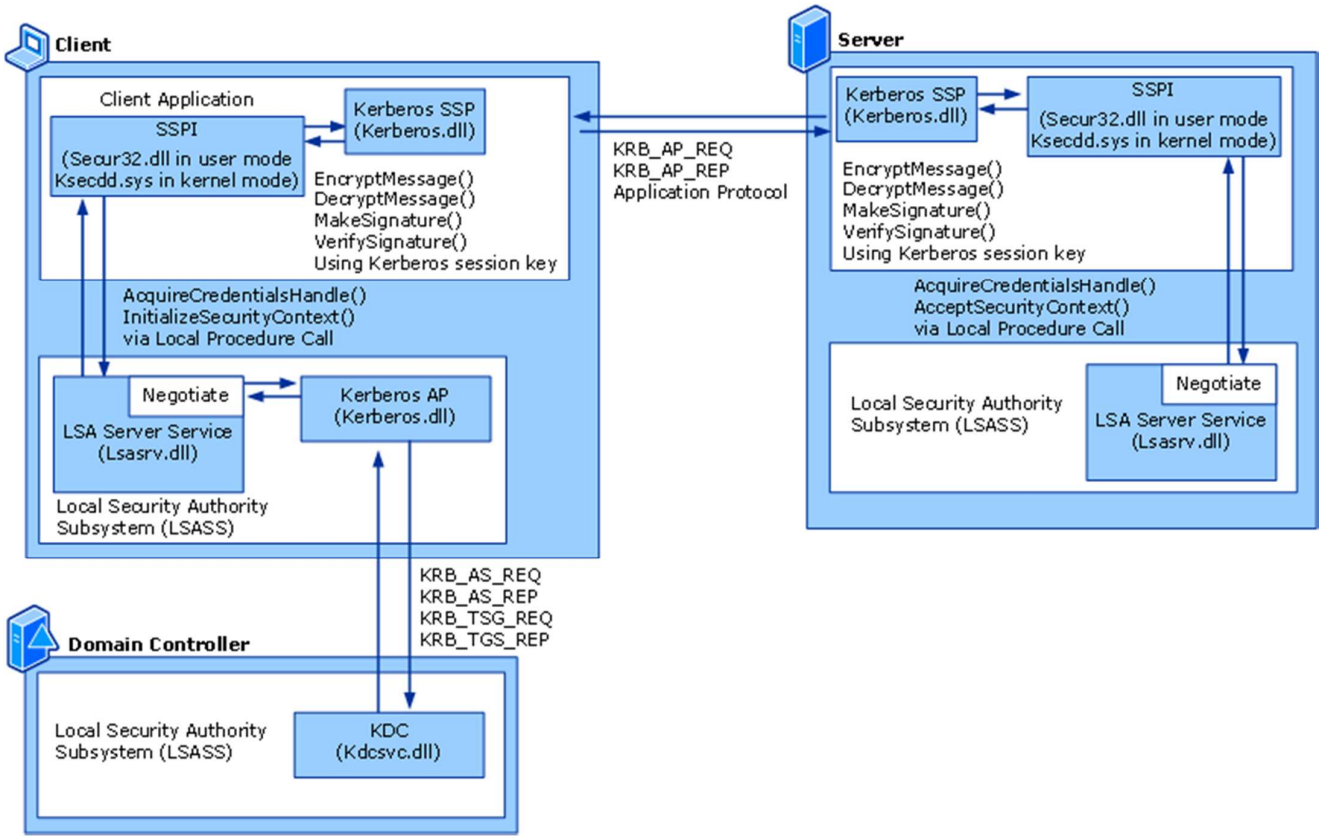


4.1.3. Kerberos: Smart Card authentication

- **Client_ID:** Security Principal Name (username, computername…)
- **[msg]key**: chiffrement de msg avec la clé key
- **K_client_pub,K_client_priv: paire de clé assymétrique**
- **K_client-TGS**: session key generated by the AS

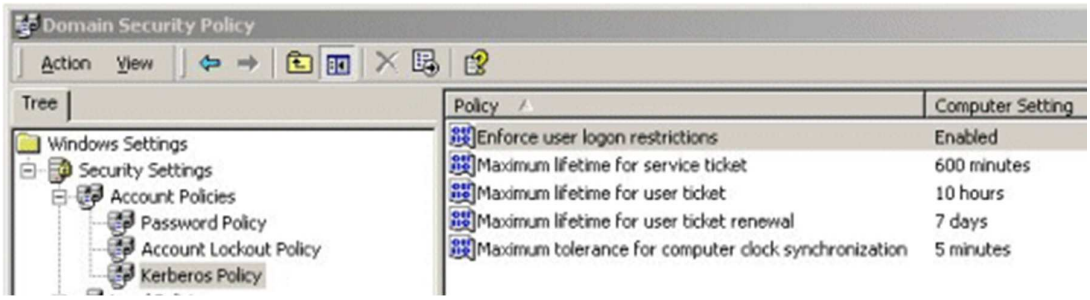


4.1.3. Kerberos et Windows: API et appels



4.1.3. Kerberos: optimisations

- **Optimisations**
  - Les tickets et le clés de sessions sont **en cache sur le client**
  - Un mécanisme permet d'obtenir des tickets sans avoir à redonner son mot de passe
    - o Ticket-Granting-Ticket (TGT) a faible durée de vie
    - o Le KDC donne des tickets sur présentation du TGT
- **Paramètres par défaut**
  - Validité TGT=10H
  - Validité TGS= 10H
  - Différence de 5 minutes MAX entre client, AS, TGS, SS ➔ synchronisation NTP



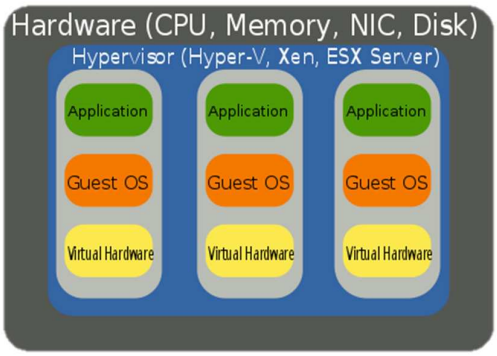
4.1.3. Kerberos – some threats and attacks

- **Threats**
  - **single-point of failure**: if only one KDC
  - **impersonation**: if at least one KDC compromised. Any user could be impersonated
- **Attacks**
  - **KDC spoofing**: old PAM_KRB5 implementation (no authorization)
  - **Replay attack**: sniff and resend 5. KRB_AP_REP
    - o KRB_AP_REP: validity duration (generally 5 minutes), source IP
    - o Service Server stores a cache of requests. Multiple identitical KRP_AP_REP are ignored
  - **Cipher**: DES (weak) initially used. Negotiation not authenticated
    - o Windows 7: DES disabled for Kerberos authentication
  - **Ticket cache attack** ("file" on the client system)
  - **Pass the Ticket**: ability to authenticate on the client. Only Microsoft implementation is vulnerable and not yet corrected.

Taming the Beast Assess Kerberos-Protected networks, Emmanuel Bouillon, *Black-Hat 2009*

4.2. Virtualisation (virtualization)

- **Mise en place d'une version virtuelle**
- **Types:**
  - **de matériel** (Hyperviseur: Hyper-V…)
  - de stockage, RAM,…
  - d'OS
  - de bureau, d'application…



HW virtualization – logical view

- **Vulnérabilités:**
  - Rajout d'une couche supplémentaire => vulnérabilité additionnelles potentielles
    - o Hyperviseur possède des droits système, sa compromission => compromission de l'ensemble des machines virtualisées sur le serveur

4.3. Conformité (conformance)

- **Définition de modèles** en fonction
  - Du type de poste (client, serveur)
  - Des besoins métiers (équipe)
  - De la politique de sécurité
- Mise en pratique des modèles
  - **agents** installés sur les postes clients et serveurs
  - Alerte en cas de non-conformité (monitoring/audit)

4.3.1. IDS / IPS

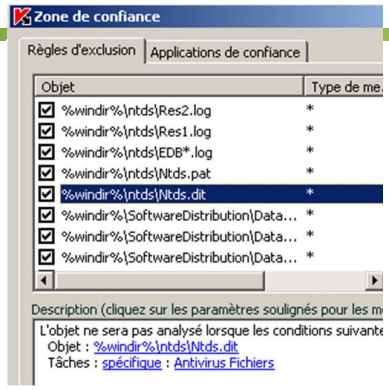
- Intrusion **Detection** System: **passif** (enregistre, notifie)
  - Composant qui monitore le réseau et/ou le système
  - Reporte les comportements suspects ou violations de politiques
- Intrusion **Prevention** System: detects and **reacts**
  - Actions automatiques ou semi-automatiques
- **Détection**
  - Comportement statistiquement anormal (métriques?)
  - Signature (attack patterns)
- **Problèmes**
  - **Faux positifs:** fausses alertes
  - **Faux négatifs:** intrusions non détectées
- **Position**
  - NIDS, NIPS: Network
  - HIDS, HIPS: Host (server, client)

4.3.2. Antimalware

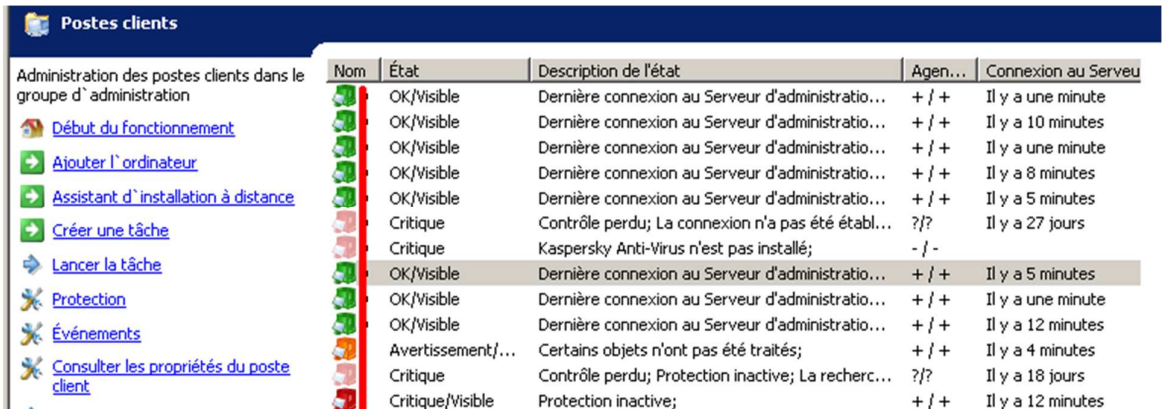
- **Détection**
  - **Classique**: “hash du binaire”
  - **Heuristiques** (intelligence artificielle)
    - **Signature générique:** Variations légères dans le code/binaire
    - **Comportement** (exécution en sandbox ou environnement virtualisé)
      - Opérations (accès fichiers, configuration du système)
      - Différences en environnement virtualisé ou non
- **!! Détection non parfaite !!** Cf théorie de Gödel sur l’incomplétude et l’incohérence. Problème INDECIDABLE
- **Configuration**
  - Centralisée
  - Selon des modèles de poste (KDC, serveur web…)
    - Exclusions (que scanner? Processus, dossiers,…)
    - Actions (autoriser, quarantaine, supprimer, demander)
    - Mises à jour de définitions
    - Scans complets du système
- **Menaces:** les antimalwares disposent de privilèges SYSTEM (iAWACS 2010)

4.3.2. Antimalware - screenshots

- **Exclusions**

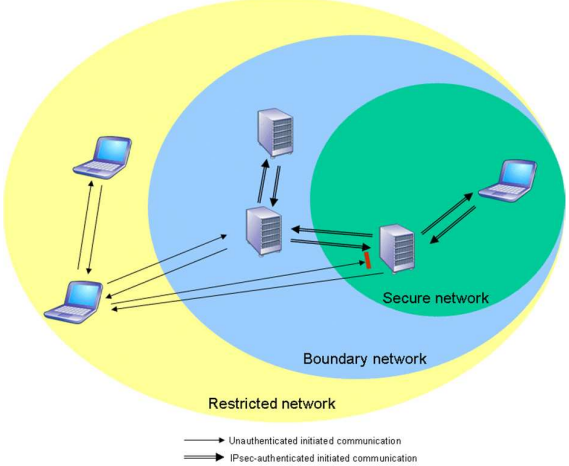


- **Monitoring**



4.3.3. Network Acces Control

- Poste client: “Accès à certaines zones” **(capacité de communication avec certaines machines)** en fonction:
  - NON de la topologie du réseau
  - Mais d’un **ensemble de métriques** du poste client
    - o Pare-feu activé?
    - o Mises à jours installées? (antimalware, OS, applications…)
    - o Chiffrement de la partition système?
    - o …
- **Méthodes d’isolation**
  - DHCP, 802.1X, VPN, IPSec
- **Produits**
  - Cisco NAC
  - Microsoft NAP (Protection)

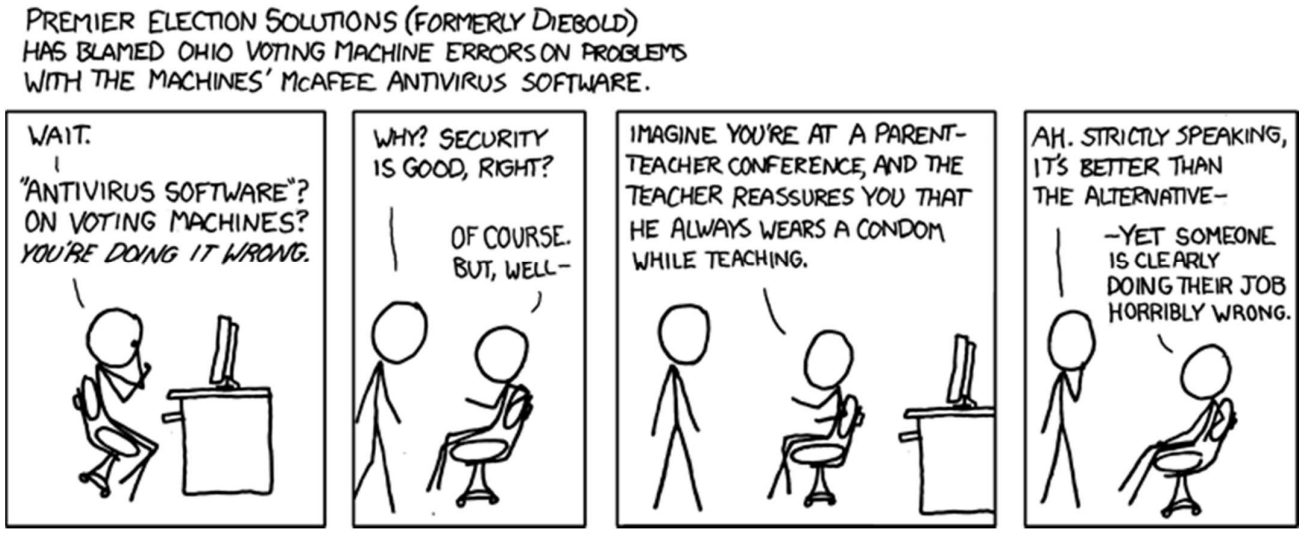


4. Intranet summary

Active Directory	Kerberos	Conformance

• Features
  • LDAP
  • DNS
  • Kerberos
• Authentication
• ACL on objects
	• Symetric cryptography
	• Single-Sign-On
	• Client wants to access a Service
	• Trusted 3rd party (KDC)
	• Asymetric crypto for Smart Card authenticaion
		• Models for computers (server, client, team, use…)
		• Intrusion Detection/Prevention Sys
		  • Attack models
		  • Undecidable problem
		• Antimalware
		  • Undecidable problem
		  • Heuristics
		• Network Access Control
		  • workstation metrics
		  • Different from topology segregation
		  • DHCP, 802.1X, IPSec…

XKCD interlude: voting machines & antimalware


PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD) HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.
WAIT. "ANTIVIRUS SOFTWARE"? ON VOTING MACHINES? YOU'RE DOING IT WRONG.
WHY? SECURITY IS GOOD, RIGHT?
OF COURSE. BUT, WELL-
IMAGINE YOU'RE AT A PARENT-TEACHER CONFERENCE, AND THE TEACHER REASSURES YOU THAT HE ALWAYS WEARS A CONDOM WHILE TEACHING.
AH. STRICTLY SPEAKING, IT'S BETTER THAN THE ALTERNATIVE-
-YET SOMEONE IS CLEARLY DOING THEIR JOB HORRIBLY WRONG.

http://xkcd.com/462/

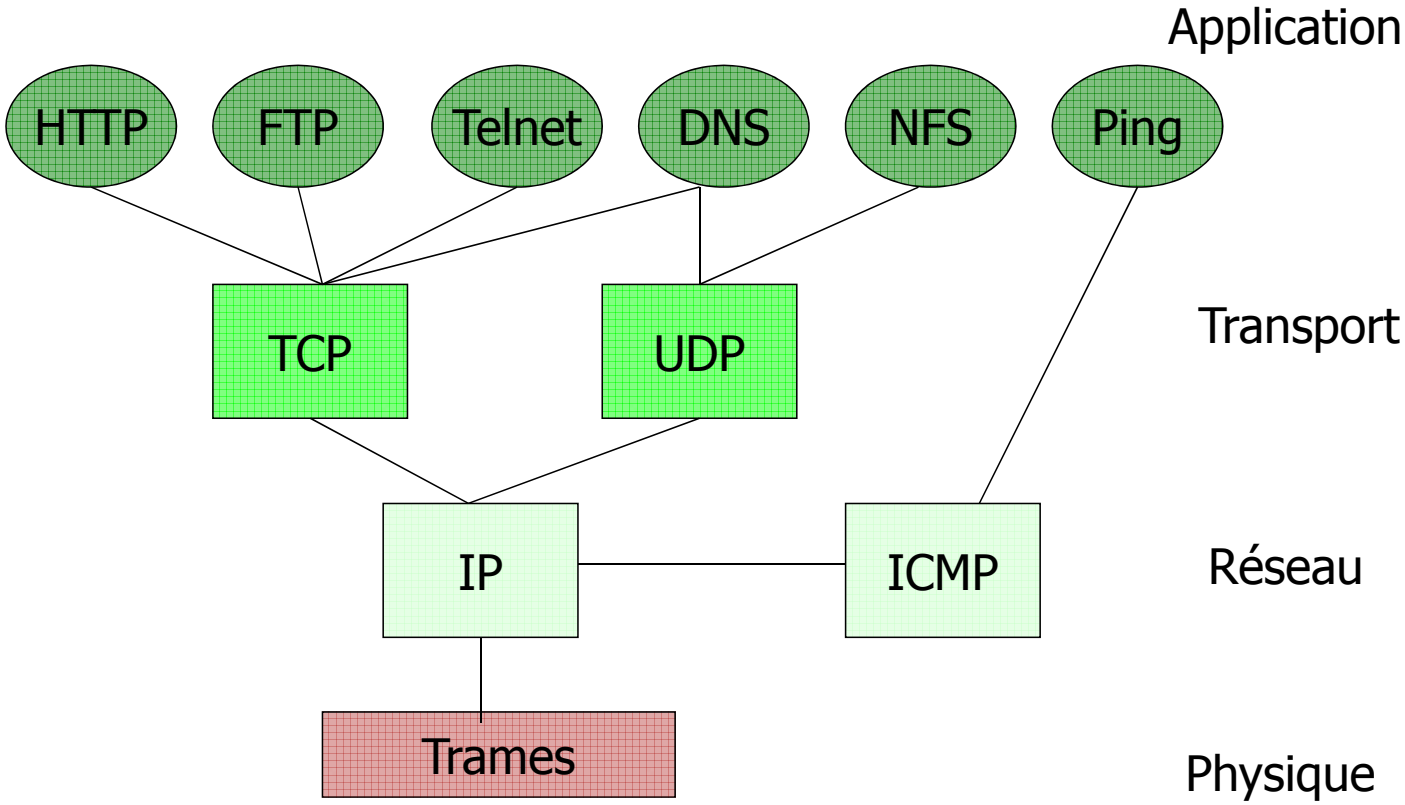
5. Accès - Protocoles

- Introduction
- IP, IPSec
- RFID
- RAS: PPP, PPTP, L2F, L2TP
- SSL/TLS
- VPN
- EAP, RADIUS
- 802.11/Wifi
- GSM

5.1. Introduction

- Les protocoles réseaux offrent dans leur implémentations natives de **nombreuses vulnérabilités**
- Tous les protocoles classiques disposent d'une version endurcie (hardened version)

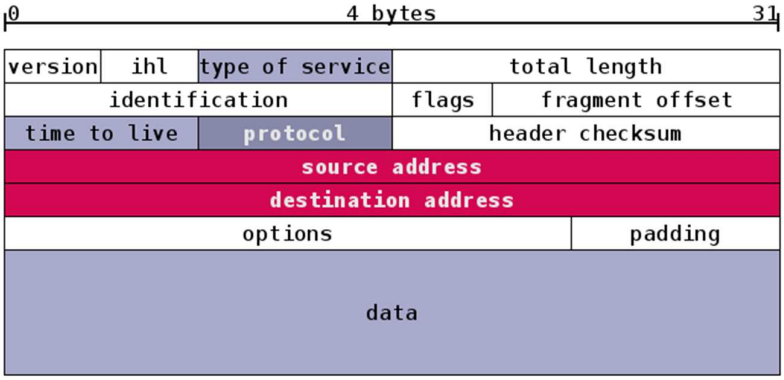
5.1. Quelques protocoles



5.1. Protocoles : IP, UDP et TCP (rappels)

- **IP : Internet Protocol (v4, v6)**
- **UDP : User Datagram Protocol**
  - Sans garantie d'ordre d'arrivée
  - Pas de retransmission
- **TCP : Transport Control Protocol**
  - Connexion garantie (circuits virtuels)
  - Correction d'erreurs
- **Cf vos Cours de réseaux!**

5.2. IPv4 – paquet (rappel)



- Un paquet IP comprend
  - Une charge (data)
  - Un Header comprenant :
    - L'adresse source IP
    - L'adresse destination IP

5.2. IPSec – extension de IPv4

- **Sécurisation de IPv4:**
  - RFC 2401 : IP Security Architecture
  - RFC 2402 : IP Authentication Header (AH)
  - RFC 2406 : IP Encapsulating Security Payload (ESP)
  - RFC 2408 : Internet Security Associations and Key Management Protocol (ISAKMP)
- **IPv6 inclus IPsec!**
  - **Cf vos Cours de réseaux!**

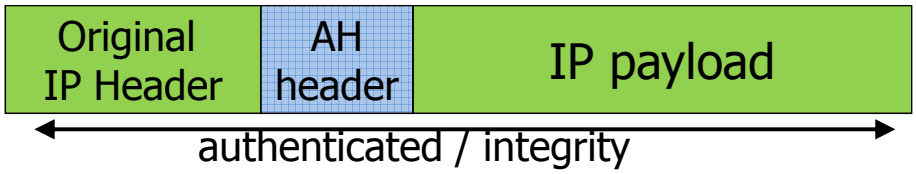
5.2. IPSec – integrity, authentication, encryption

- **AH** (51st IP protocol)
  - Authentication, integrity, anti-replay
  - **NO CONFIDENTIALITY**
  - integrity on PAYLOAD and IP header
    - o problems with Network Address Translation **(Network lectures)**
- **ESP** (50th IP protocol)
  - Authentication, integrity, anti-replay
  - **PAYLOAD CONFIDENTIALITY**
  - IP header unchanged only in tunnel mode
  - NAT-Transversal
- **Usages: AH, ESP or AH+ESP**

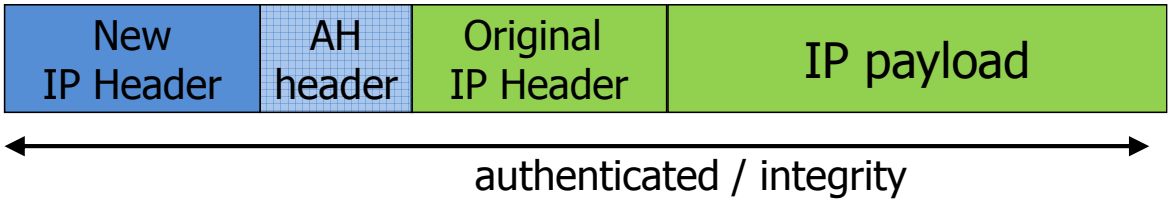
Formation DirectAccess, Youssef Zizi & Cyril Voisin, Microsoft (2010)

5.2. IPSec Authentication Header (AH)

- **Transport mode**



- **Tunnel mode**

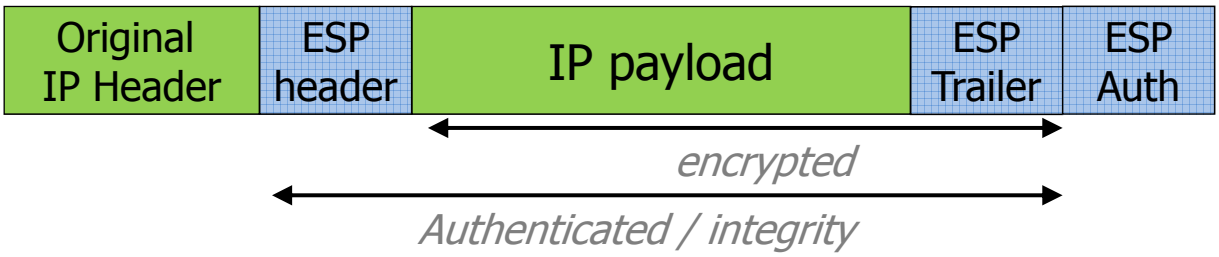


- **Integrity:** hash covering the whole datagram, except
  - TypeOfService, Fragment Offset, Flags, TTL, IP header checksum

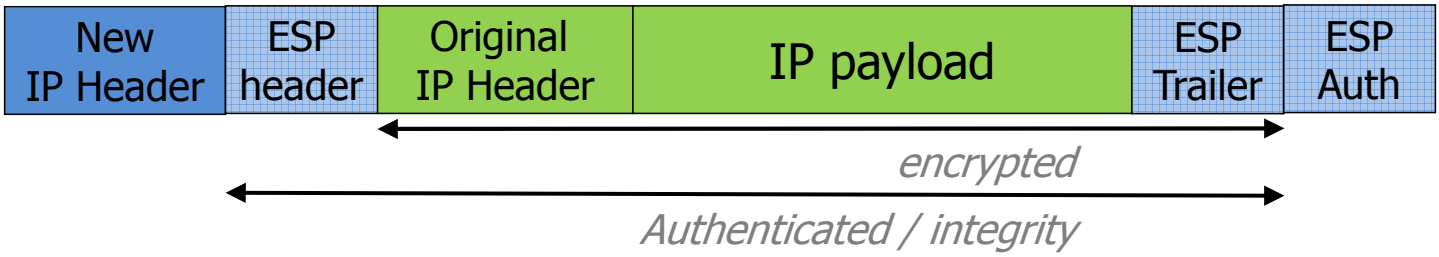
Formation DirectAccess, Youssef Zizi & Cyril Voisin, Microsoft (2010)

5.2. IPSec Encapsulating Security Payload (ESP)

- **Transport mode**



- **Tunnel mode**



- IP header NOT protected

Formation DirectAccess, Youssef Zizi & Cyril Voisin, Microsoft (2010)

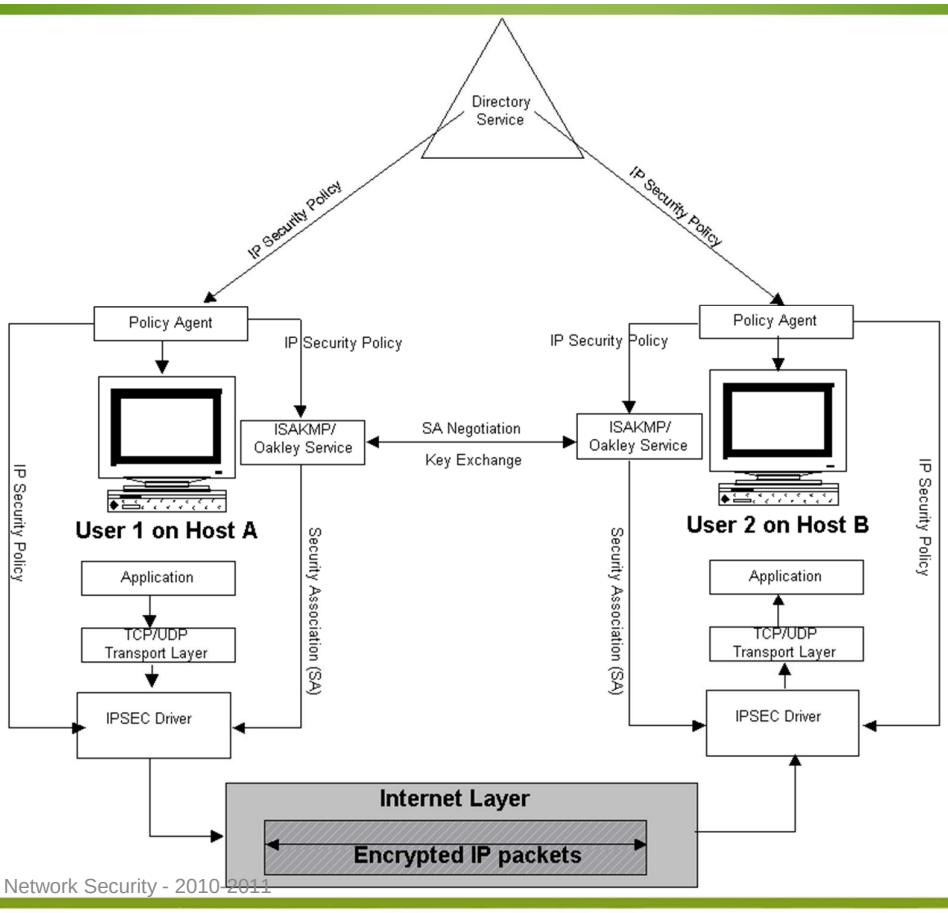
5.2. IPSec – SA & IKE

- **SA : Security Association**
  - Décrit comment seront utilisés les services de sécurité lors d'un échange
    - o L'algorithme de **chiffrement** utilisé
    - o L'algorithme d'**authentification** utilisé
    - o Une **clé de session partagée** (donc symétrique, pour raison de performance)
  - unidirectionnel
  - lie des adresses IP

Vue des SA dans le pare-feu Windows (NT6+, Vista et ultérieur)

- **IKE : Internet Key Exchange**
  - Distribution des clés

5.2. IPSec en entreprise



ECOLE NATIONALE SUPERIEURE D'INFORMATIQUE ET DE MATHEMATIQUES APPLIQUEES

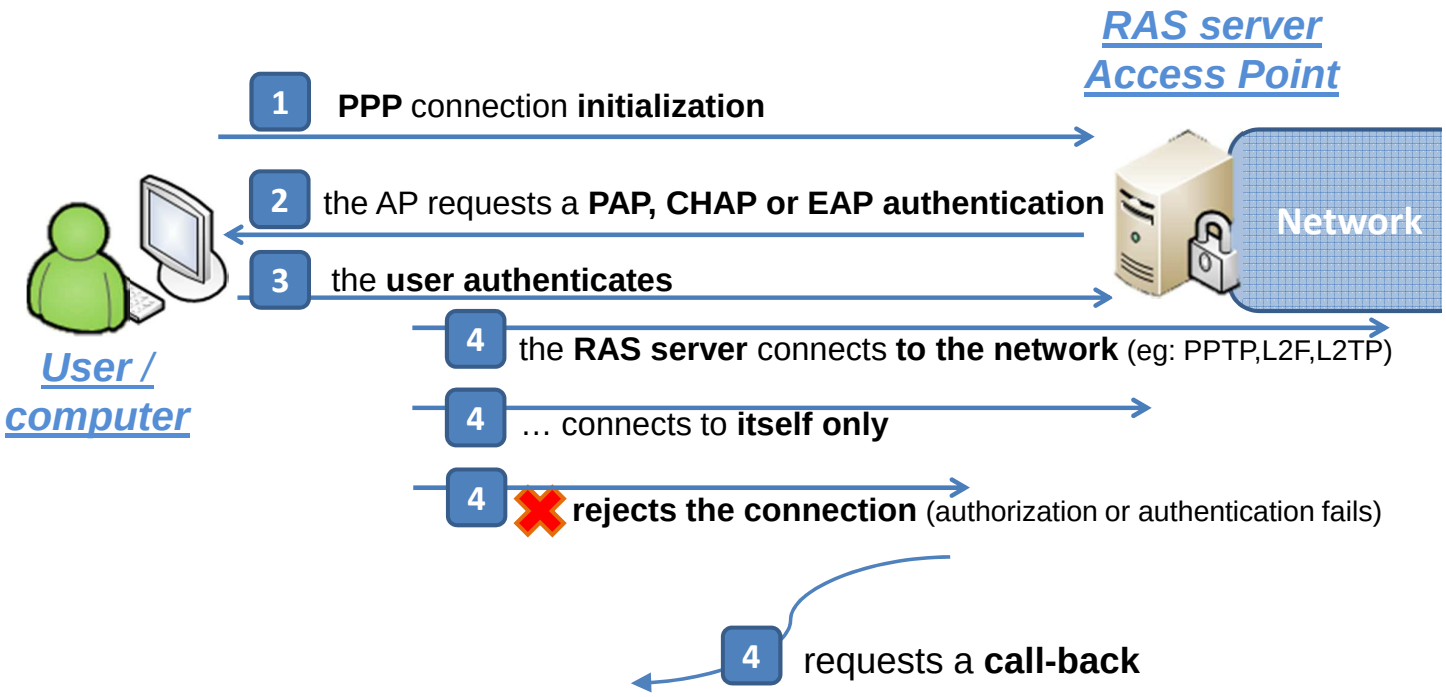
5.3. Radio Frequency IDentification "RFID"

- Reader + tag(s)
- tag ; two main types:
  - only replies its **ID** (cleartext, without reader authentication nor data encryption)
  - can perform **cryptographic operations**
- **Applications**: Tracking (Passport, goods), Access control
- **Security issues**:
  - **Privacy** (eg: chip inside hand, contactless)
  - Vulnerabilities:
    - **Replay** attacks (if no cryptoprocessor)
    - Wireless, thus **antenna range** (amplification..) => privacy
    - The ID is generally used within a web application (thus classic **web attacks** (SQL injection, XSS…)) => check your Conceiving Web-App lectures

ECOLE NATIONALE SUPERIEURE D'INFORMATIQUE ET DE MATHEMATIQUES APPLIQUEES

5.4. Remote Access Server « RAS »

- Permits a remote access to IP and IPX networks
- May eventually require a Call-Back

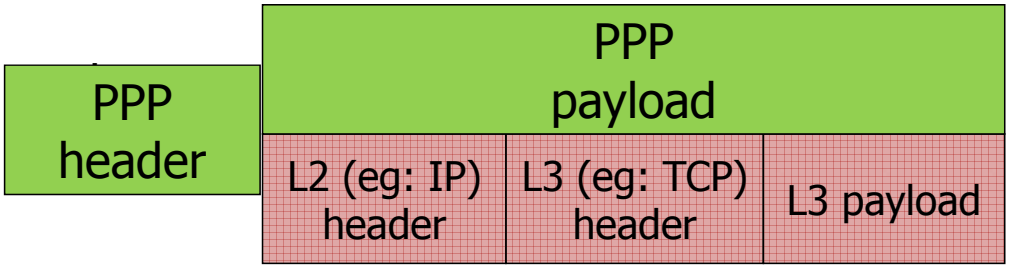

RAS server
Access Point
1 PPP connection initialization
2 the AP requests a PAP, CHAP or EAP authentication
3 the user authenticates
Network
4 the RAS server connects to the network (eg: PPTP,L2F,L2TP)
4 … connects to itself only
4 rejects the connection (authorization or authentication fails)
User / computer
4 requests a call-back

5.4.1. Point-to-Point Protocol "PPP"

- **Data link protocol** for a communication between **two nodes** ***"Point-to-Point connection"***
- Authentication, encryption, compression
- Connection to a **Remote Access Server**

Application	FTP SMTP HTTP …	DNS ; …
Transport	TCP	UDP
Internet	IP ; IPv6	
Network access	PPP	
	PPPoE	PPPoA
	Ethernet	ATM

- PPP: dialup ; PPPoE & PPPoA : DSL
- RFC: http://tools.ietf.org/html/rfc1661
- PPP

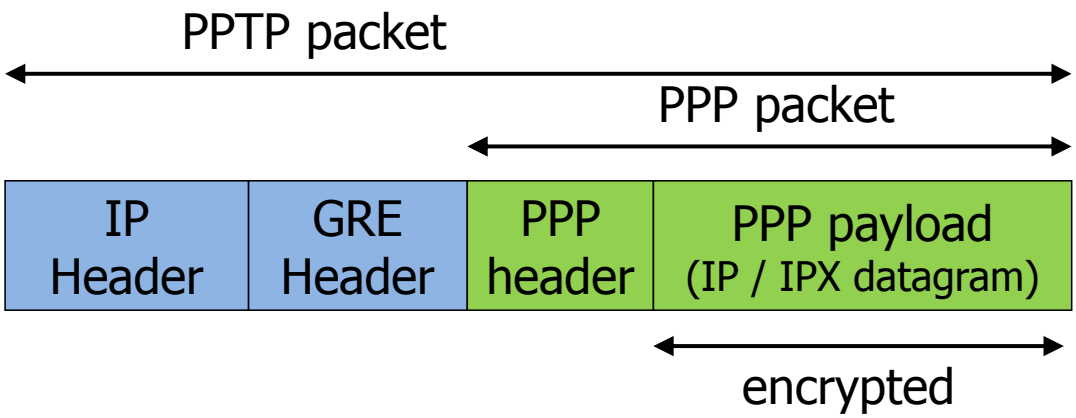


5.4.2. RAS Authentication methods

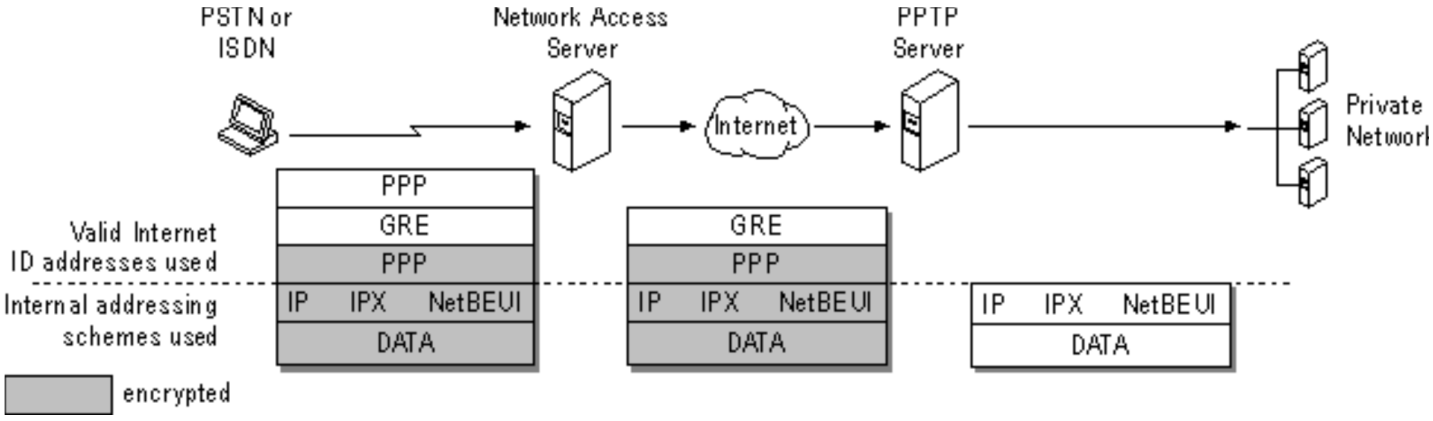
- **PAP (Password** Authentication Protocol)
  - **unencrypted ASCII password !**
- **CHAP (Challenge Handshake** AP)
  - Shared secret key (eg: user password)
  - Periodically a challenge is sent to the client
  - Response: hash(challenge,secret_key)
- **EAP (Extensible** AP)
  - several authentication methods
    - EAP-TLS

5.4.3. Tunnel protocols: PPTP

- **PPTP : Point-to-Point Tunelling Protocol**
  - Microsoft (& Alcatel-Lucent, 3Com)
  - PPP link **over IP ONLY**
    - GRE Generic Routine Encryption tunnel encapsulating PPP packets
    - Control channel over TCP 1723
  - permits confidentiality, integrity and authentication



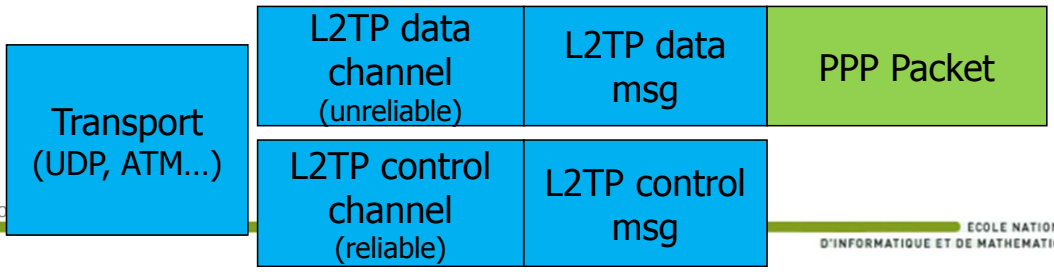
5.4.3. PPTP data flow



5.4.3. Tunnel protocols: L2F, L2TP

- These ones have **no encryption capabilities**
  - Necessary to use an additional protocol (eg: IPSec)
- **L2F : Layer 2 Forwarding protocol**
  - Cisco, 1998 RFC2341
  - UDP 1701

- **L2TP : Layer 2 Tunelling Protocol**
  - 1999, Cisco & Microsoft RFC2661, L2TPv3 2005 RFC3931
  - Not necessarily over an IP network ; does support RADIUS

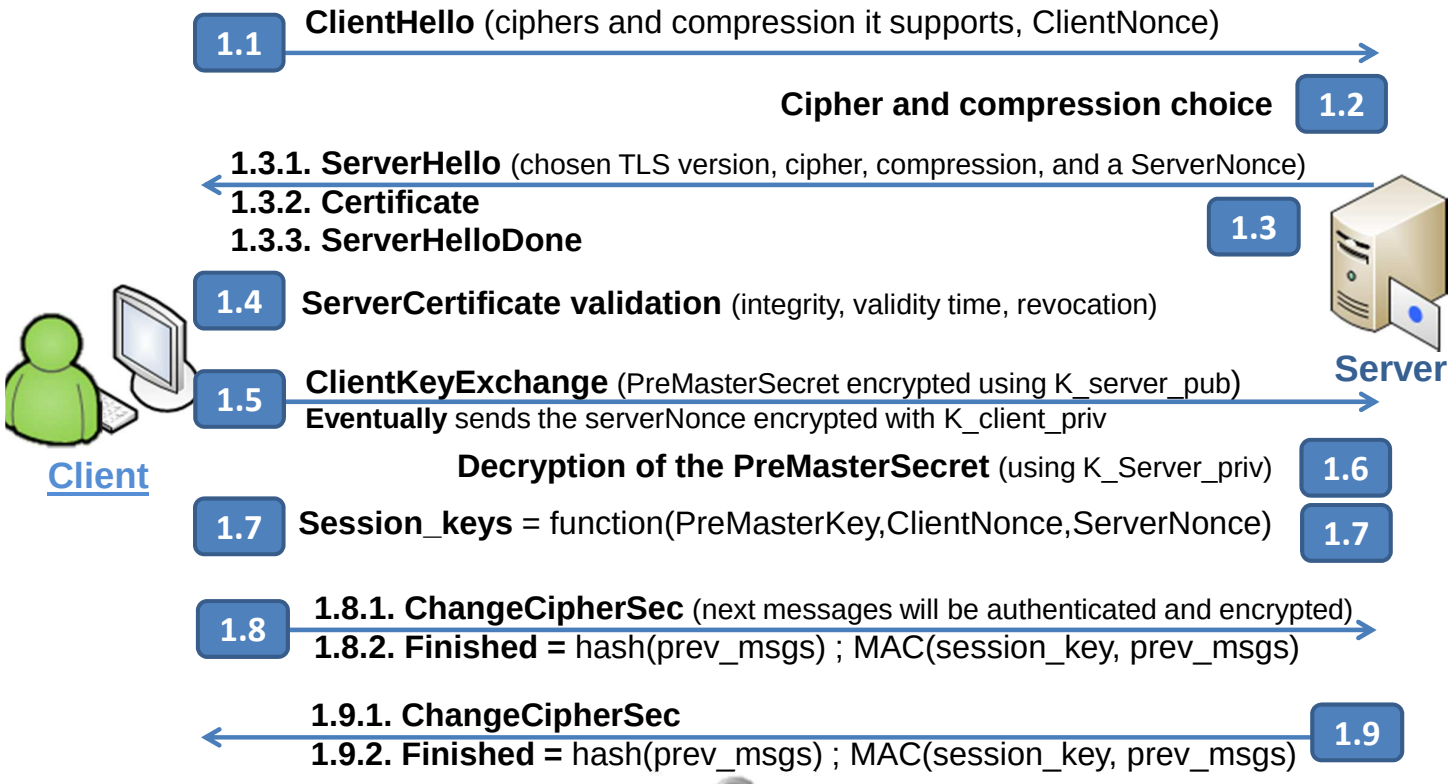


5.5. Secure Socket Layer "SSL" / TLS

- SSL 1.0: Netscape, 1995 ; TLS = Transport Security Layer
- Current version: **TLS 1.2 (aka SSL 3.3),** RFC5248 **aug 2008**
- Security properties
  - o **Communication:**
    - **Integrity (MAC)**
    - **Confidentiality (symmetric cryptography)**
  - o **Server: authentication (asymetric crypto)**
  - o **Key exchange** (RSA, Diffie-Hellman…)
  - o **Eventually client authentication**
- Sub-protocols
  - o **Handshake**: version, algorithm, authentication
  - o **Record**: data fragmentation (app. layer), integrity, confidentiality
  - o **Alert**: errors, end of session
  - o **ChangeCipherSpec**: messages will be authenticated (and eventually encrypted)
  - o **Application**: application data

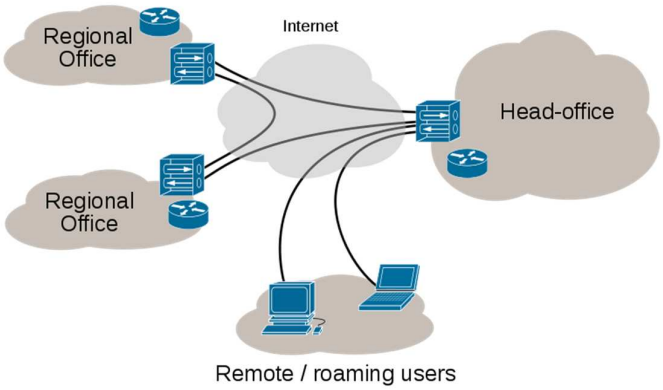
5.5. SSL handshake (unauthenticated client)

MAC = Message Authentication Code ; hash_function(key, message)


1.1 ClientHello (ciphers and compression it supports, ClientNonce)
Cipher and compression choice 1.2
1.3.1. ServerHello (chosen TLS version, cipher, compression, and a ServerNonce)
1.3.2. Certificate
1.3.3. ServerHelloDone
1.3
1.4 ServerCertificate validation (integrity, validity time, revocation)
Server
1.5 ClientKeyExchange (PreMasterSecret encrypted using K_server_pub)
Eventually sends the serverNonce encrypted with K_client_priv
Client
Decryption of the PreMasterSecret (using K_Server_priv) 1.6
1.7 Session_keys = function(PreMasterKey,ClientNonce,ServerNonce) 1.7
1.8 1.8.1. ChangeCipherSec (next messages will be authenticated and encrypted)
1.8.2. Finished = hash(prev_msgs) ; MAC(session_key, prev_msgs)
1.9.1. ChangeCipherSec
1.9.2. Finished = hash(prev_msgs) ; MAC(session_key, prev_msgs) 1.9

5.6. Virtual Private Network (VPN)

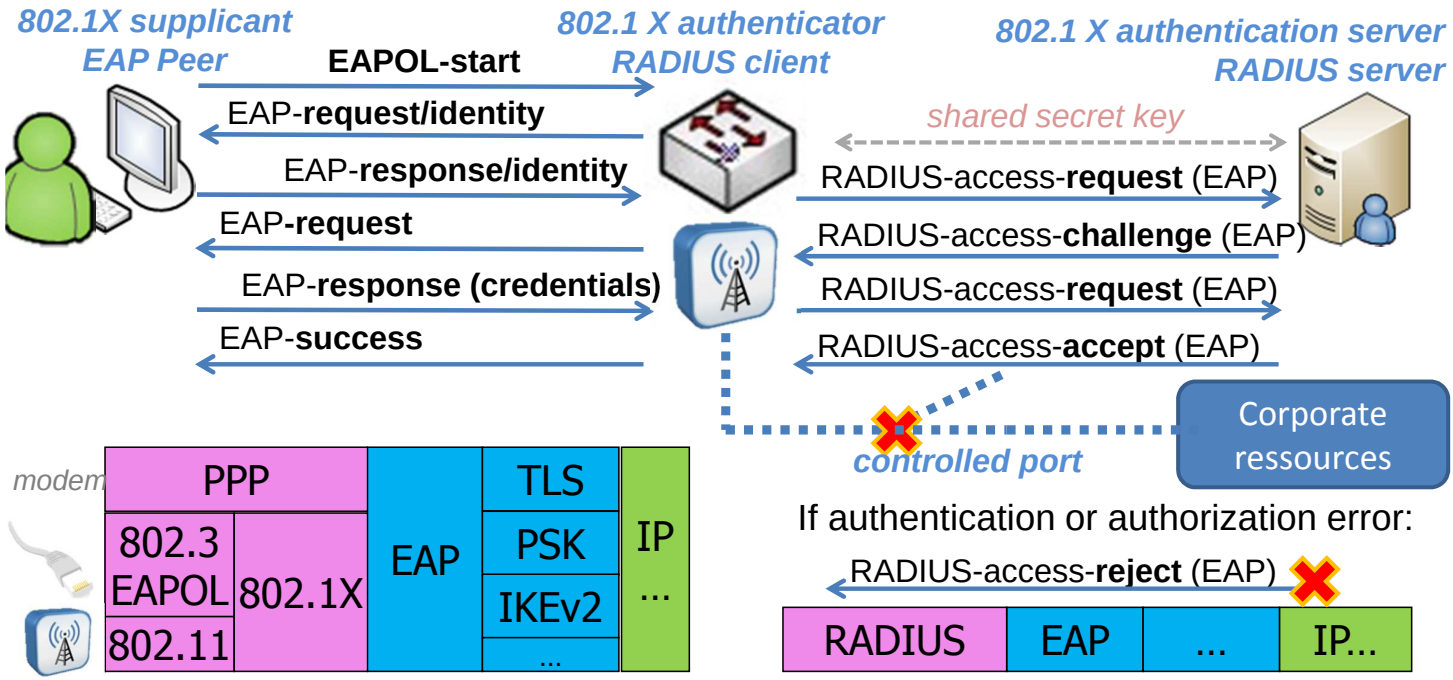
- Réseau Privé Virtuel
- **Private (confidential) tunnel over a public network**
  - Interconnecting with remote office
  - Connecting to the corporate network when outside



- **Protocols**
  - PPTP, L2TP/IPSec
  - HTTPS
- **Risks**
  - "the Internet can access inside the corporate network"
    - o strong authentication (at least 2 factors)
    - o operational network teams, security teams

5.7. 802.1X, EAP, RADIUS

- **EAP, authentication** framework RFC5247
- Used in 802.1X, PPP ; could use **RADIUS for authorization**



5.8. 802.11 - Wifi

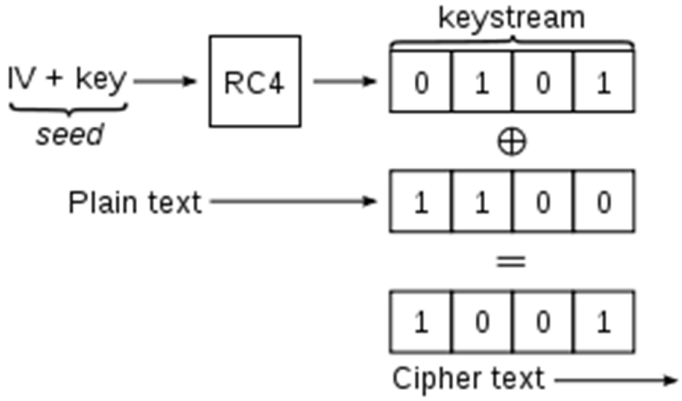
- **802.11 security**
  - 802.11
  - RC4
  - WEP
  - SKA
- **WPA**
- **802.11i**
  - WPA2
- **802.11 security in corporations**

5.8.1. 802.11

- 802.11: a (1999), b(1999), g(2003), n (2009)
- Review your network courses
- Security (1999):
  - **Data encryption:** Wireless Equivalent Privacy “WEP”
  - **Authentication:**
    - Shared Key Authentication “SKA” (WEP is used during authentication)
    - Open System Authentication (no authentication occurs)

5.8.1. Reminder: RC4

- stream cipher
- **IV**: Initialisation Vector
- **Key** (shared between the parties)



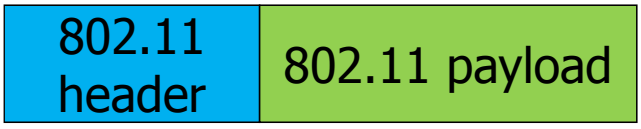
[Wikipedia-WEP]

- **Flaws**:
  - if the same IV is used, same as one-time pad!
  - if number generator weak, ability to gain some knowledge about the key

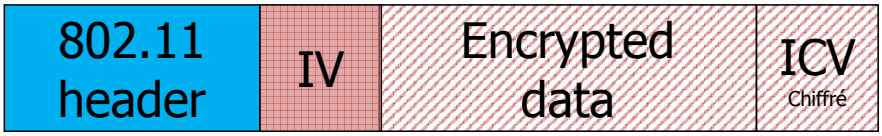
[Weaknesses in the Key Scheduling Algorithm of RC4], *Scott Fluhrer, Itsik Mantin, Adi Shamir*

5.8.1. Wireless Equivalent Privacy "WEP"

- Chiffre = RC4 – 56 bits
- **IV :** 24 bits
  - 802.11 does not prevent reusing the same IV!!
- **Key = "WEP password"**
  - 40 bits (40+24= "64 bits WEP security")
  - 104 bits ("128 bits WEP security")
- **ICV : Integrity Check Value** : CRC-32
- clear-text frame:

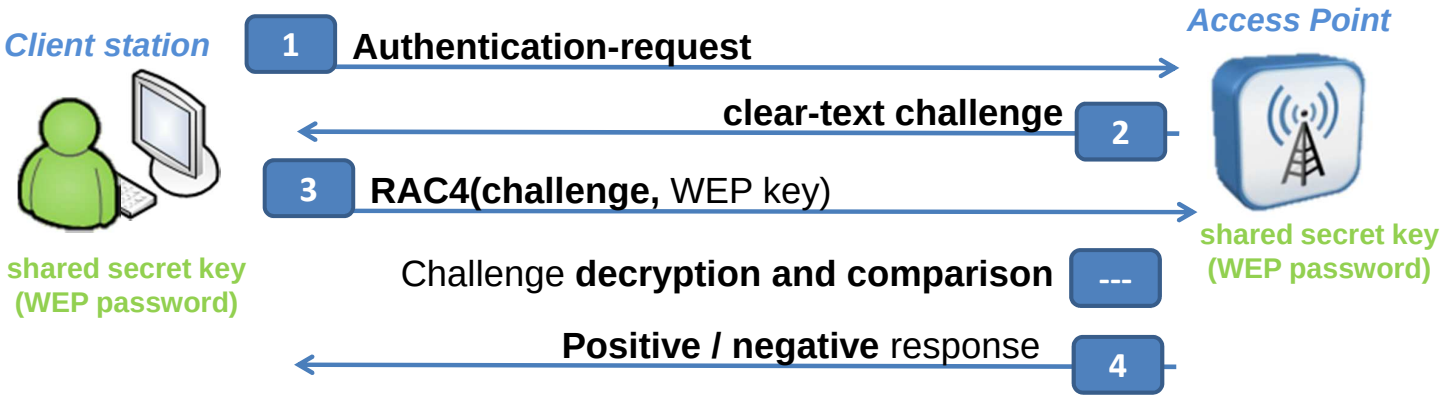


- **WEP-encrypted frame:**



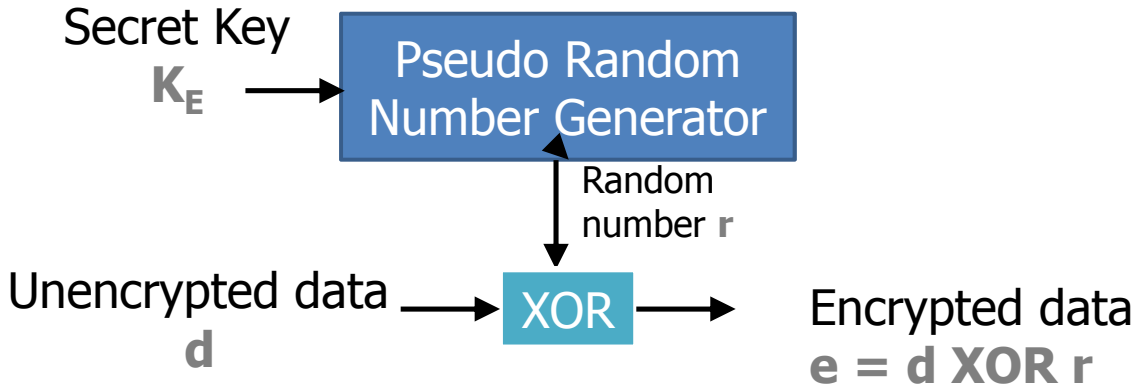
5.8.1. Shared Key Authentication “SKA”

- **Four Way Handshake** using the WEP password (secret key)



5.8.1. RC4 problem – Vernam cipher

- if real randomness, then one-time pad



- **What if r is not so random?...**

5.8.1. Stream cipher: basic cryptanalysis

- **What if the same encryption key is used at least two times?**
  - e1=d1 XOR r
  - e2=d2 XOR r
  - Then: e1 XOR e2 = d1 XOR d2
- **From that we can deduce:**
  - reusing r is a VERY bad idea
  - **d1 and d2 are not random (thus sensible to "patterns attacks". See aircrack (ARP attacks))**
  - **802.11**
    - **ICV (CRC) could confirm we did find the value!**
    - **"r" is IV+wep_password**

5.8.1. the Birthday paradox with 802.11 IVs

- **Pn**: probability that 2 packets among n do use the same IV
  - IV: 24 bits ; thus number of IV = 2^24
  - $P_2 = 1/(2^{24})$
  - $P_n = P_{n-1} + (n - 1)(1 - P_{n-1})/(2^{24})$ (n>2)
- Pn >= 50%
  - Starting from only **n=4823 packets**!

5.8.1. WEP security?

- **Attacking WEP only takes ~ 3 minutes**
  - **aircrack-ng** (original work, Christophe Devine)
- **Consequences**
  - Ability to modify the packets (integrity loss)
  - Ability to authenticate
- **Solutions**
  - **increasing** the size of the WEP key (and/or the possible space of the IV) is not enough (B'day paradox)
  - authentication, we could use **EAP** (see 802.11 WPA2)
  - we should rely on **another kind of cipher** (eg: block cipher, see WPA)

5.8.2. Wifi Protected Access "WPA"

- Intermediate measures to protect Wifi networks while waiting for full **802.11i specs (aka WPA2)**
  - 2002
  - without changing the hardware! (only require a ram flash)
- **Authentication and integrity**
  - **Temporary Key Integrity Protocol (TKIP)**
    - still RC4 but: 128 bits key/packet
    - rekeying mechanism (frequently change, avoiding collisions)
    - the ICV field is replaced by
      - a MICHAEL integrity check (64 bits)
      - sequence number for each packet (replay protection)
  - **AES (block cipher), optionnal**
    - Mandatory in WPA2

5.8.2. WPA (with TKIP) attacks

- En novembre **2008** deux chercheurs allemands en sécurité, Éric Tews et Martin Beck, ont annoncé avoir découvert une faille de sécurité dans le protocole WPA. La **faille, située au niveau de l'algorithme TKIP (Temporal Key Integrity Protocol),** exploite l'architecture du protocole WPA.
- TKIP se met en place après le protocole WEP, or le code MAC est contenu dans un paquet WEP, ce qui permet à un pirate informatique de l'intercepter. Une fois intercepté le paquet peut être utilisé pour récupérer le code MAC et se faire passer pour le point d'accès. Cette méthode est encore plus efficace en interceptant les paquets ARP puisque leur contenu est connu. (attaques par pattern).Cette faille concerne exclusivement le protocole WPA utilisant TKIP. **Les protocoles utilisant AES restent sécurisés.**
- Les détails concernant cette faille ont été exposés de façon détaillée durant la conférence PacSec les 12 et 13 novembre 2008 à Tokyo[2]. Martin Beck a intégré l'outil pour exploiter cette faille dans son outil de piratage des liaisons sans fil, nommé aircrack-ng (createur originel d'aircrack: Christophe Devine).
- **Contre-mesure: Il est toutefois assez facile de contrevenir à cette faille en forçant la négociation des clés toutes les deux minutes ce qui ne laisse pas assez de temps pour que l'attaque réussisse.**

5.8.3. 802.11i

- IEEE standard: 802.11-2007 (draft in 2004, amended in 2007)
- **WPA2**
  - **CCMP (Counter-Mode/CipherBlockChaining-Mac Protocol)**
    - o AES/FIPS-197
    - o 128-bit key, 128 bits cipher block
    - o 10 rounds of encoding
  - **802.1x** support in 802.11
  - **Key distribution**

5.8.4. 802.11 in corporations

- WPA-enterprise
- **WPA2-enterprise**

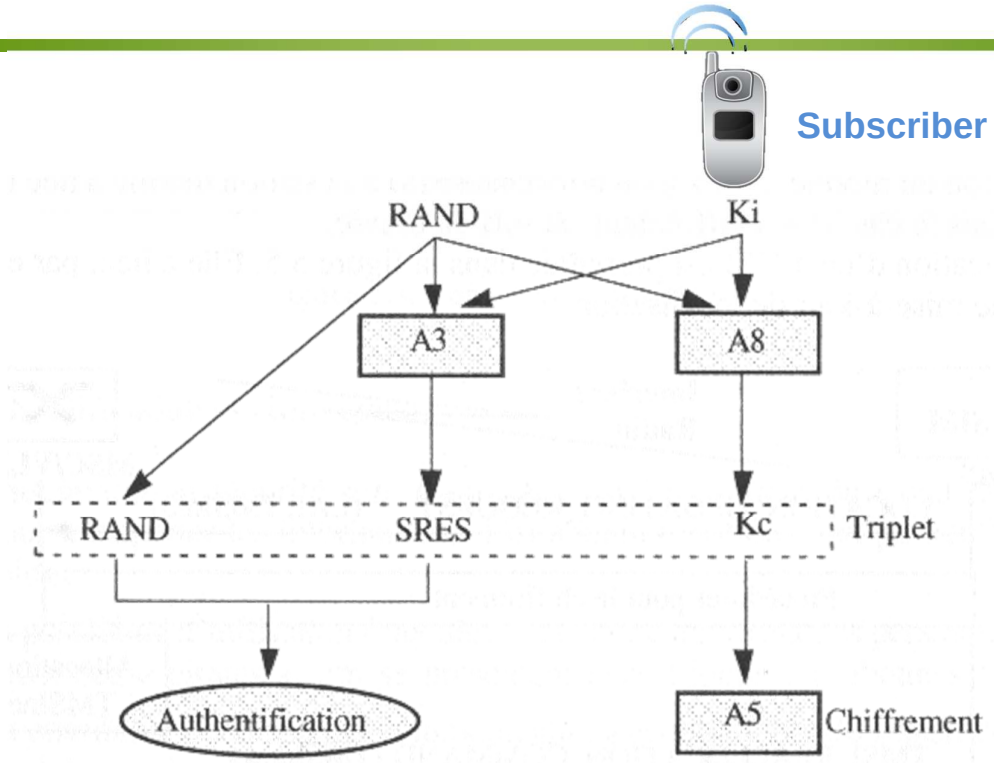
- **EAP** for authentication and encryption. Mostly used
  - **EAP-TLS (with certificates, thus a PKI is needed)**
  - EAP-TTLS
  - PEAP (Microsoft)

5.9. GSM

- **5 billion users**
- For the basics, review your 1st year GSM course

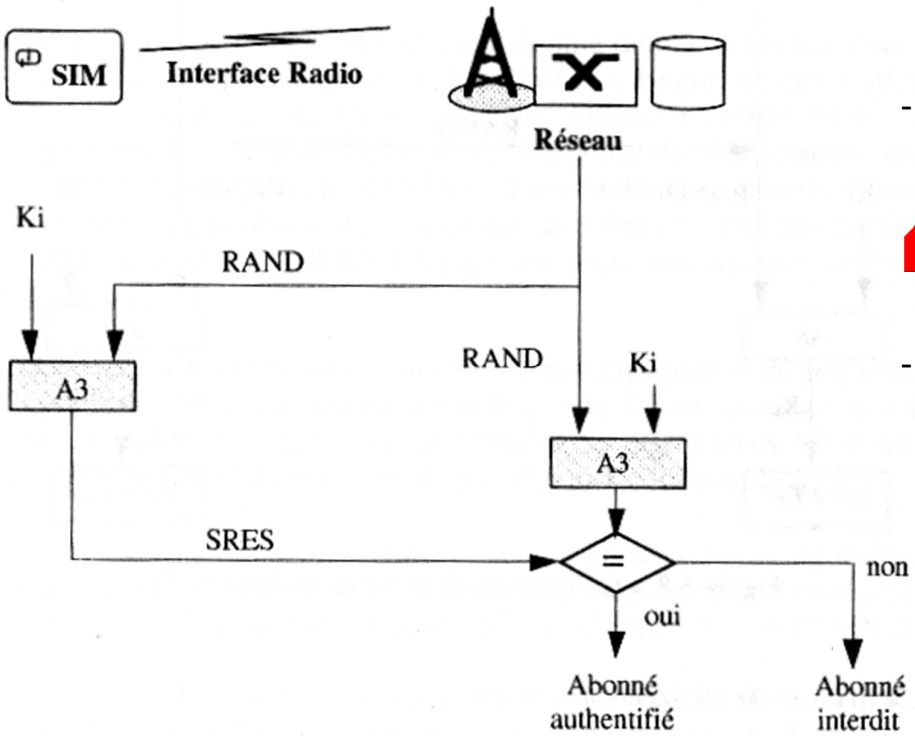
- Main security services
  - Subscriber **authentication**
  - **Data** and signalization **confidentiality**
  - Subcriber **identity confidentiality / (privacy)**

5.9. GSM security – global view



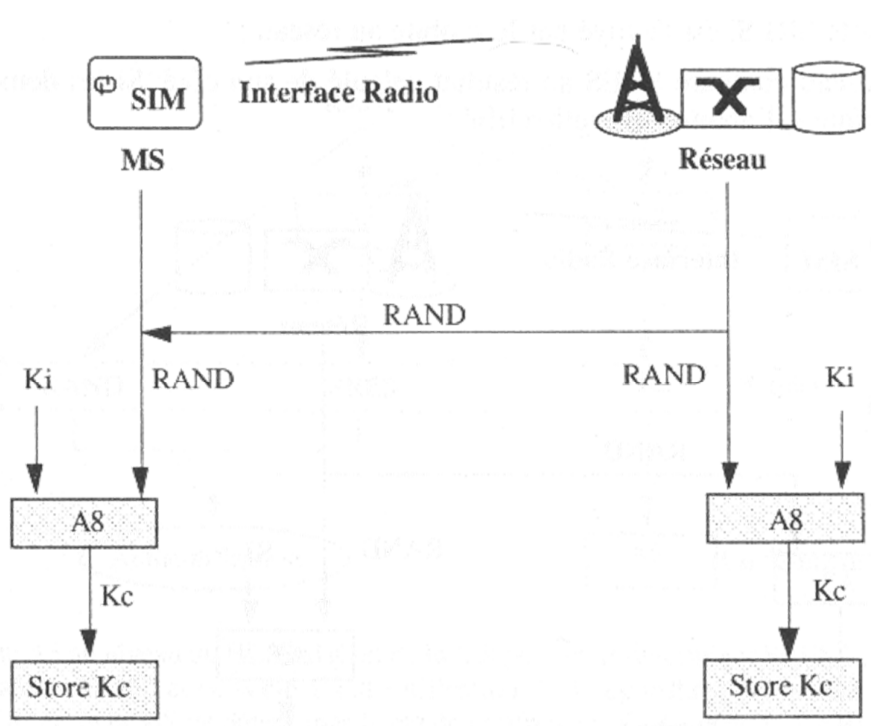
- Le triplet (RAND,SRES,K_c) est passé d'un réseau à l'autre
- A5, algorithme de chiffrement, n'est toujours pas officiellement public (A5/1, A5/3)
- A3 + A8 est connu sous le nom de A38

5.9. GSM security – subscriber authentication



- Le réseau envoit un challenge RAND
- L'**abonné possède une clé secrète Ki**
  - Stockée dans la carte SIM et dans l'AUC (Centre d'authentification)
- L'**authentification** sert à générer une clé **Kc** de **chiffrement des données et de la signalisation**
  - **A3: one-way hash** paramétré par clé

5.9. GSM security – data and signalization confidentiality

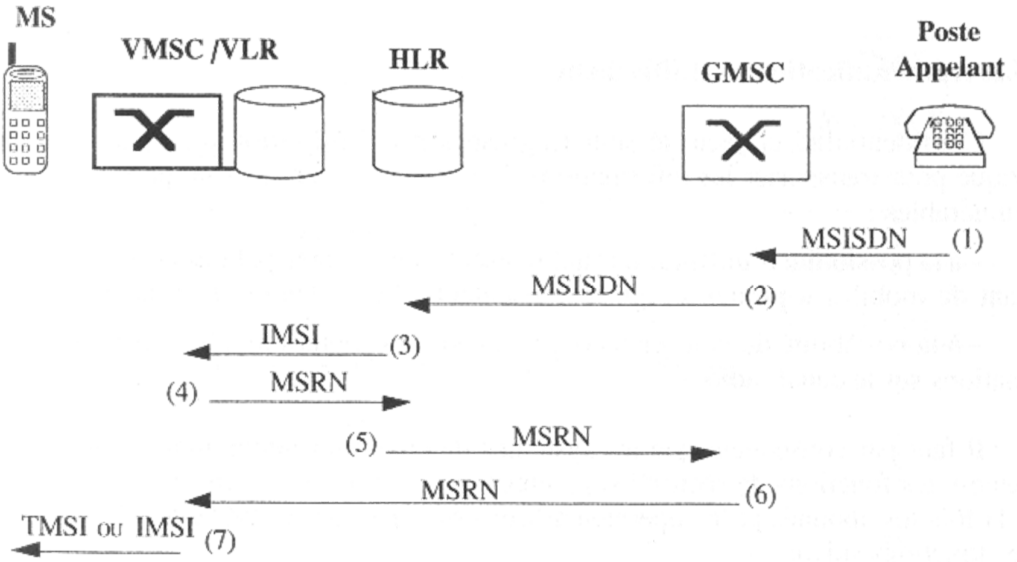


- **A8**
  - Le réseau et le mobile
    - **Kc=A8(Ki,RAND)**
    - One-way hash paramétrée par clé
- **A5=symetric stream cipher** (specs secrètes)
  - chiffre les **données et la signalisation**
  - **A5/1** (initially USA+Europe)
  - **A5/2** (initially others)
  - **A5/3** ***(should be used everywhere…)***

5.9. GSM security – protecting the subscriber identity

- **Identification de l'abonné (MS): seul le numéro est connu**
  - **IMSI** : Identité invariante de l'abonné : est gardée secrète à l'intérieur du réseau
  - **TMSI : Identité temporaire, attribuée après une authentification réussie**
  - **MSISDN** : Numéro de l'abonné : c'est le seul identifiant de l'abonné mobile connu à l'extérieur du réseau GSM
  - **MSRN** : Numéro attribué lors d'un appel, pour l'acheminement des données

5.9. GSM security – protecting the subscriber identity



Note :
- VLR : Visitor Location Register : registre de la cellule ou se trouve le mobile
- HLR : Home Location Register : registre de l'opérateur du mobile
- VMSC : Visitor Mobile Service Switching Center : établissement, hand-over et SMS
- GSMC : Gateway SMC

5.9. GSM security – subscriber privacy

- **Frequency-Hopping Speard Spectrum (FHSS)**
  - Rapidly switching of carrier among many channels
  - Using a pseudorandomness function

- Usage
  - Mainly for QoS
  - .. But could and **SHOULD be used for user privacy!**

5.9 attacking the wideband GSM network

- **Cryptosystem**
  - **"A5/1 could be cracked in seconds"** *GSM SRLSY? Karsten Nohl, 26C3 (2010)*
    - 2To rainbow tables (…available on Bittorrent)
    - … for less than $1.000 H/W! *Wideband GSM Sniffing, Karsten Nohl, Sylvain Munaut, 27C3 (2011)*
  - A5/3
    - *A practical-Time attack on the A5/3 Cryptosystem Used in 3G telephony, Orr Dunkelman, Nathan Keller et Adi Shamir (2010)*
    - 75% probability with 1Go of data. ~ 2H communication. (seems unpractical)
    - However, since multimedia usage do proliferate…

- **…And in practise:**
  - Unfrequent TMSI changes
  - Unfrequent Hopping
  - No systematic rekeying before each call or SMS
  - Predictable padding => confidentiality threatened!!

5.9. GSM security in 2011…

GSM should currently be used as an untrusted network, just like the Internet

Threat	Investment	Scope	Mitigation
Fake base station	Low	Local	Mutual authenti-cation & trust anchor
Passive intercept of voice + SMS	Low	Local	
Passive intercept of data	Currently not possible		
Phone virus / malware	Medium to high	Large	Trust anchor
Phishing	High	Large	

Cell phone networks do not provide state-of-the art security.

Protection must be embedded in the phones and locked away from malware.

Wideband GSM Sniffing, Karsten Nohl, Sylvain Munaut, 27C3 (2011)

5. Protocols, access summary

IPSec
- Useful for VPN and for internal network
- Modes: transport, tunnel
- AH, ESP, IKE, SA

EAP
- Authentication framework
- 802.1X, RADIUS, WPA(2)-enterprise

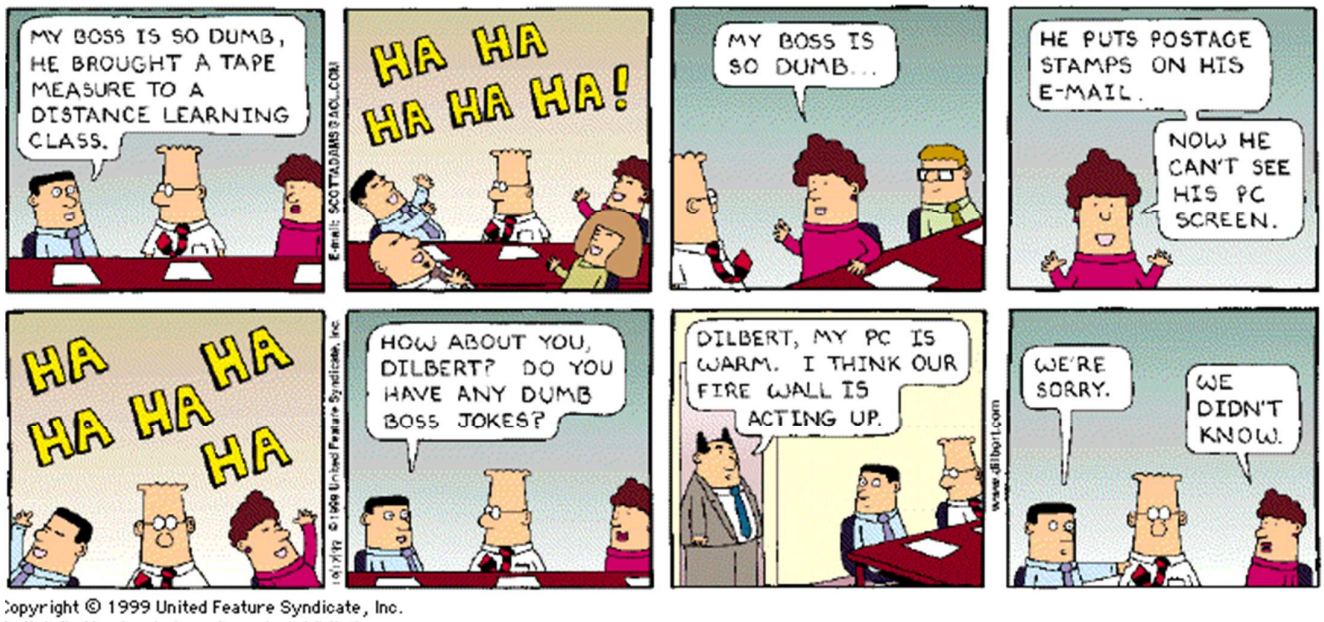
VPN
- Encrypted tunnel over a public network
- IPSec, L2TP/IPSec, L2F, HTTPS

SSL/TLS
- Btwn transport and application layer
- Certificate (server, eventually client)
- handshake

802.11
- WEP: RC4 stream cipher
- WPA: adds TKIP, not enough
- WPA2: AES block cipher
- Corporations: WPA(2)-enterprise ; mostly EAP-TLS

GSM
- TMSI: temporary identity
- Hopping: mainly for QoS (could be for privacy)
- Rekeying each time the user authenticate
- A5/1, A5/2: should not be used (real-time attacks)

Interlude


MY BOSS IS SO DUMB, HE BROUGHT A TAPE MEASURE TO A DISTANCE LEARNING CLASS.
HA HA HA HA HA!
MY BOSS IS SO DUMB...
HE PUTS POSTAGE STAMPS ON HIS E-MAIL.
NOW HE CAN'T SEE HIS PC SCREEN.
HA HA HA HA HA HA
HOW ABOUT YOU, DILBERT? DO YOU HAVE ANY DUMB BOSS JOKES?
DILBERT, MY PC IS WARM. I THINK OUR FIRE WALL IS ACTING UP.
WE'RE SORRY.
WE DIDN'T KNOW.
www.dilbert.com
Copyright © 1999 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited.